

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## **IMAGES ARE BEST AVAILABLE COPY.**

As rescanning documents *will not* correct images,  
Please do not report the images to the  
Image Problem Mailbox.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yoichi KANAI ET AL

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: SYSTEM, METHOD AND COMPUTER READABLE MEDIUM FOR CERTIFYING RELEASE OF  
ELECTRONIC INFORMATION ON INTERNET

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	11-341288	NOVEMBER 30, 1999
JAPAN	11-341289	NOVEMBER 30, 1999

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and  
(B) Application Serial No.(s)
  - ☐ are submitted herewith
  - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

*Surinder Sachar*

Gregory J. Maier  
Registration No. 25,599

Surinder Sachar  
Registration No. 34,423



22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 10/98)



#5  
3-12-01  
JM

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

JC918 U.S. PTO  
09/725515  
11/30/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1 9 9 9 年 1 1 月 3 0 日

出 願 番 号

Application Number:

平成 1 1 年 特 許 願 第 3 4 1 2 8 8 号

出 願 人

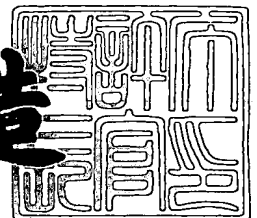
Applicant (s):

株式会社リコー

2 0 0 0 年 9 月 1 日

特 許 庁 長 官  
Commissioner,  
Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2 0 0 0 - 3 0 7 0 3 3 1

【書類名】 特許願

【整理番号】 9907601

【提出日】 平成11年11月30日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00  
G06F 12/14

【発明の名称】 電子情報公開証明方法及びシステム、並びに電子情報公開証明プログラムを格納した記憶媒体

【請求項の数】 28

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号  
株式会社 リコー内

【氏名】 金井 洋一

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号  
株式会社 リコー内

【氏名】 谷内田 益義

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号  
株式会社 リコー内

【氏名】 水野 富夫

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号  
株式会社 リコー内

【氏名】 古川 達也

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号  
株式会社 リコー内

【氏名】 石川 洋一

【特許出願人】

【識別番号】 000006747

【氏名又は名称】 株式会社 リコー

【代表者】 桜井 正光

【手数料の表示】

【予納台帳番号】 003724

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子情報公開証明方法及びシステム、並びに電子情報公開証明プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項 1】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法であって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報をコピーするステップと、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性情報を記憶装置に格納するステップと、

前記記憶装置に格納された前記電子証明書及び前記属性情報を当該証明依頼元に提供するステップと、

を含むことを特徴とする電子情報公開証明方法。

【請求項 2】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法であって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングでアクセスし、アクセスするごとに前記特定の電子情報をコピーする第 1 ステップと、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性情報を記憶装置に格納する第 2 ステップと、

を含むことを特徴とする電子情報公開証明方法。

【請求項 3】 前記電子証明書に対応して、最初にコピーされた前記特定の電子情報を記憶装置に格納する第 3 ステップをさらに含むことを特徴とする請求項 2 記載の電子情報公開証明方法。

【請求項 4】 前記記憶装置に格納された前記電子証明書及び前記属性情報を証明依頼元に提供する第 4 ステップをさらに含むことを特徴とする請求項 2 記載の電子情報公開証明方法。

【請求項 5】 前記第 4 ステップが、前記電子証明書に対応する前記特定の電子情報を前記証明依頼元に提供するステップを含むことを特徴とする請求項 4 記載の電子情報公開証明方法。

【請求項 6】 前記第 1 ステップが、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングで且つアクセス元のアドレスを変更しつづつアクセスするステップを含むことを特徴とする請求項 2 記載の電子情報公開証明方法。

【請求項 7】 前記第 1 ステップが、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングで且つ所定の頻度でアクセスするステップを含むことを特徴とする請求項 2 記載の電子情報公開証明方法。

【請求項 8】 前記特定の電子情報をアクセス可能とするための参照情報を前記特定のコンピュータ以外の前記ネットワークに接続されたコンピュータに保持させるステップをさらに含むことを特徴とする請求項 2 記載の電子情報公開証明方法。

【請求項 9】 コピーされた前記特定の電子情報の変更の有無を検出するステップと、

変更があることを検出した場合には、当該変更があったということを記憶装置に格納するステップと、

をさらに含むことを特徴とする請求項 2 記載の電子情報公開証明方法。

【請求項 10】 前記記憶装置に格納された前記特定の電子情報を検索可能なように前記ネットワーク上の前記特定のコンピュータ以外のコンピュータで公開するステップをさらに含むことを特徴とする請求項 3 記載の電子情報公開証明方法。

【請求項 11】 前記記憶装置に格納された前記特定の電子情報の要約を検索可能なように前記ネットワーク上の前記特定のコンピュータ以外のコンピュータで公開するステップをさらに含むことを特徴とする請求項 3 記載の電子情報公

開証明方法。

【請求項 1 2】 前記特定の電子情報が前記ネットワーク上で提供されている電子情報検索手段により検索可能である場合には、当該検索可能であるということを記憶装置に格納するステップをさらに含むことを特徴とする請求項 2 記載の電子情報公開証明方法。

【請求項 1 3】 前記ネットワークがインターネットであり、  
前記電子情報はマークアップ・ランゲージにより記述された文書であり、  
前記ネットワーク上における前記電子情報の所在に関する情報はユニフォーム・リソース・ロケータであり、  
前記アクセス条件は、少なくともアクセス元の IP アドレスを含むことを特徴とする請求項 2 記載の電子情報公開証明方法。

【請求項 1 4】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムであって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報をコピーする手段と、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性電子情報を記憶装置に格納する手段と、

前記記憶装置に格納された前記電子証明書及び前記属性電子情報を提供する手段と、

を有することを特徴とする電子情報公開証明システム。

【請求項 1 5】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムであって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報へ所定のタイミングでアクセスし、アクセスするごとに前記特定の電子情報をコピーするアクセス手段と、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニ



ークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性情報を記憶装置に格納する手段と、

前記記憶装置に格納された前記電子証明書及び前記属性情報を当該証明依頼元に提供する発行手段と、

を有することを特徴とする電子情報公開証明システム。

【請求項 1 6】 前記電子証明書を発行する手段をさらに有することを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 1 7】 前記記憶装置が、前記電子証明書に対応して、最初に取得された前記特定の電子情報のコピーを格納することを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 1 8】 前記提供手段が、前記電子証明書に対応する、前記記憶装置に格納された前記特定の電子情報を前記証明依頼元に提供することを特徴とする請求項 1 7 記載の電子情報公開証明システム。

【請求項 1 9】 前記アクセス手段が、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングで且つアクセス元のアドレスを変更しつつアクセスすることを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 2 0】 前記アクセス手段が、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングで且つ所定の頻度でアクセスすることを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 2 1】 前記特定の電子情報をアクセス可能とするための参照情報を格納し、前記ネットワークに接続した、前記特定のコンピュータ以外のコンピュータ をさらに含むことを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 2 2】 コピーされた前記特定の電子情報の変更の有無を検出し、変更があることを検出した場合には、当該変更があったということを前記記憶装置に格納する手段をさらに有することを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 2 3】 前記特定の電子情報を格納し且つ検索可能とする、前記ネ

ットワークに接続した、前記特定のコンピュータ以外のコンピュータをさらに有することを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 2 4】 前記特定の電子情報の要約を格納し且つ検索可能とする、前記ネットワークに接続した、前記特定のコンピュータ以外のコンピュータをさらに有することを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 2 5】 前記記憶装置が、前記特定の電子情報が前記ネットワーク上で提供されている電子情報検索手段により検索可能である場合には、当該検索可能であるということを格納することを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 2 6】 前記ネットワークがインターネットであり、  
前記電子情報はマークアップ・ランゲージにより記述された文書であり、  
前記ネットワーク上における前記電子情報の所在に関する情報はユニフォーム・リソース・ロケータであり、  
前記アクセス条件は、少なくともアクセス元の IP アドレスを含むことを特徴とする請求項 1 5 記載の電子情報公開証明システム。

【請求項 2 7】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するためのプログラムを格納した記憶媒体であって、

前記プログラムは、

前記特定のコンピュータ以外のコンピュータに、記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報をコピーするステップと、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性情報を記憶装置に格納するステップと、

前記記憶装置に格納された前記電子証明書及び前記属性情報を当該証明依頼元に提供するステップと、

を含むことを特徴とする記憶媒体。

【請求項 2 8】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するためのプログラムを格納した記憶媒体であって、

前記プログラムは、

前記特定のコンピュータ以外のコンピュータに、記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングでアクセスし、アクセスするごとに前記特定の電子情報をコピーする第 1 ステップと、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性情報を記憶装置に格納する第 2 ステップと、

を含むことを特徴とする記憶媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明が属する技術分野】

本発明は、ネットワーク上の電子情報が公開されていたことを証明するための方法、システム及びプログラム並びに該プログラムを格納した記録媒体に関する。

【0 0 0 2】

【従来の技術】

従来から、ある電子情報が特定の日に存在していたことを認証する方法及びシステムは存在していた。このような方法及びシステムは、例えば米国特許第 5 1 3 6 6 4 7 号、米国再審査特許第 R E 3 4 9 5 4 号、米国特許第 5 1 3 6 6 4 6 号、米国特許第 5 3 7 3 5 6 1 号、米国特許第 5 7 8 1 6 2 9 号などに記載されている。

しかし上述の米国特許に示された技術は、例えばインターネット等で、特定の電子情報が公開されていたことを証明するものではない。

【0 0 0 3】

【発明が解決しようとする課題】

近年、インターネット等でも技術情報が開示されるようになり、このような技術情報は、雑誌や図書等の形で刊行された技術情報と同等の内容の情報を含んでおり、その伝達の迅速性等は従来の刊行物とは比較にならないほどである。よって、研究者が自己の研究成果を早期に公表すること等を目的としてインターネット等を使用することも多くなっている。また、従来の刊行物に比して情報の発信が簡便であり、コストも低いため、より多くの情報がインターネット等で公開される可能性が高い。しかし、従来技術では電子情報が存在していたことを証明することはできるが、インターネット等で公開されていたということを証明することはできなかった。すなわち、電子情報が秘密であったかどうかを判別することができなかった。

斯かる場合、即ちインターネット等で公開されていたということを証明することができない場合には、公開されていた技術内容と同様の内容の特許を他人が取得してしまうという恐れがある。上述の通り、インターネット等で公開された技術情報は、実質的に刊行物と同じ効果を奏するものであり、日本においては「電子通信回線を通じて公衆に利用可能になった発明」に対しては特許を与えないような法律が制定されている。しかし、インターネット等で公開された技術情報は、いつ公開されていたのか、改ざんされていないのか、という事実を証明することが困難であるため、証拠としての信頼性が従来の刊行物に比して弱い、という面は否めない。

そこで、本発明は、インターネット等のネットワーク上で、ある特定の電子情報が所定の条件の下公開されていたことを証明するための方法、システム及びコンピュータ・プログラム並びに該コンピュータ・プログラムを格納した記録媒体を提供することを目的とする。

【 0 0 0 4 】

【課題を解決するための手段】

本発明の第 1 の態様に係る、ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法は、記録依頼に応じて、特定のコンピュータに格納された当該特定の電子情報にアクセスし、特定の電子情報をコピーするステップと、コピーされた特定の電子情報及びネットワー

ク上における特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性情報を記憶装置に格納するステップと、記憶装置に格納された電子証明書及び属性情報を当該証明依頼元に提供するステップとを含む。これにより、証明書の日時で且つ属性情報に含まれる所在に関する情報（例えばURL（Uniform Resource Locator））で指定された場所の電子情報にアクセスできたことが証明できるようになる。

本発明の第2の態様に係る電子情報公開証明方法は、記録依頼に応じて、特定のコンピュータに格納された前記特定の電子情報に所定のタイミングでアクセスし、アクセスするごとに特定の電子情報をコピーする第1ステップと、コピーされた特定の電子情報及びネットワーク上における特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性情報を記憶装置に格納する第2ステップとを含む。このようにすれば、電子情報が一定期間ネットワーク上で公開されていることを合わせて証明できるようになる。

また、本発明の第2の態様において、電子証明書に対応して、最初にコピーされた当該特定の電子情報を記憶装置に格納する第3ステップをさらに含むような構成も可能である。記録依頼元で電子情報を保管しておくことも可能であるが、本実施態様においては、証明書等と共に一元管理するようにしている。

さらに、本発明の第2の態様において、記憶装置に格納された電子証明書及び属性情報を当該証明依頼元に提供する第4ステップをさらに含むような構成も可能である。

また、上で述べた第4ステップを、電子証明書に対応する当該特定の電子情報を証明依頼元に提供するステップを含むように構成することも可能である。

また、上で述べた第1ステップを、特定のコンピュータに格納された特定の電子情報に所定のタイミングで且つアクセス元のアドレスを変更しつつアクセスするステップを含むように、又は特定のコンピュータに格納された特定の電子情報に所定のタイミングで且つ所定の頻度でアクセスするステップを含むように構成することも可能である。アクセス元アドレスの変更を行うことにより、不特定の

コンピュータからアクセスできることの証明ができるようになる。また、所定の頻度でアクセスすることにより、電子情報の変更などについて捕捉し易くなる。

【0005】

本発明の第2の態様において、特定の電子情報をアクセス可能とするための参照情報を特定のコンピュータ以外のネットワークに接続したコンピュータに保持させるステップをさらに含むように構成することも可能である。この参照情報によって一般公衆が電子情報の所在を容易に得ることができるようになり、電子情報の公衆による利用可能性を向上することができる。この参照情報が存在することも何らかの形で証明できるようにすることが好ましい。

また本発明の第2の態様において、コピーされた当該特定の電子情報の変更の有無を検出するステップと、変更があることを検出した場合には、当該変更があったということを記憶装置に格納するステップとをさらに含むような構成も可能である。これにより、電子情報のバージョン遷移の記録が可能になる。

さらに本発明の第2の態様において、記憶装置に格納された電子情報を検索可能のようにネットワーク上の当該特定のコンピュータ以外のコンピュータで公開するステップをさらに含むような構成も可能である。電子情報の公衆による利用性をより高めることができ、さらに第三者も証明書付の電子情報を使用することができるようになる。これに関連して、記憶装置に格納された電子情報の要約を検索可能のようにネットワーク上の当該特定のコンピュータ以外のコンピュータで公開するステップをさらに含むような構成も可能である。

本発明の第2の態様において、前記特定の電子情報をネットワーク上で提供されている電子情報検索手段により検索が可能である場合には、当該検索が可能であるということを記憶装置に格納するステップをさらに含むような構成も可能である。その特定の電子情報を電子情報検索手段により検索が可能であるということは、公衆による利用可能性が非常に高いことを意味しており、この事実により当該特定の電子情報の証拠力は飛躍的に高まることとなる。

なお、上で述べたネットワークにはインターネットが最も適用し易く、その場合、電子情報はHTML (Hyper Text Markup Language)、XML (eXtensible Markup Language) 等のマークアップ・ランゲージにより記述された文書であり

、ネットワーク上における電子情報の所在に関する情報はユニフォーム・リソース・ロケータ（URL）であり、アクセス条件は、少なくともアクセス元のIPアドレスを含むとすることが可能である。

## 【0006】

本発明の第3の態様に係る、ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムは、記録依頼に応じて、特定のコンピュータに格納された当該特定の電子情報へアクセスし、特定の電子情報をコピーする手段と、コピーされた特定の電子情報及びネットワーク上における特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性電子情報を記憶装置に格納する手段と、記憶装置に格納された電子証明書及び属性電子情報を提供する手段とを有する。

また、本発明の第4の態様に係る電子情報公開証明システムは、記録依頼に応じて、特定のコンピュータに格納された特定の電子情報へ所定のタイミングでアクセスし、アクセスするごとに特定の電子情報をコピーするアクセス手段と、コピーされた特定の電子情報及びネットワーク上における特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性情報を記憶装置に格納する手段と、記憶装置に格納された電子証明書及び属性情報を当該証明依頼元に提供する発行手段とを有する。

本発明の第4の態様において、電子証明書を発行する手段をさらに有するような構成も可能である。

なお、本発明の第2の態様について説明した第2の態様の変形例を、第4の態様に係る電子情報公開証明システムに対して応用することも可能である。

さらに、本発明の第1及び第2の態様に係る電子情報公開証明方法をコンピュータで実行するためのプログラムとして実装することが可能であり、このプログラムは、例えばフロッピー・ディスク、CD-ROM、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。

## 【0007】

## 【発明の実施の形態】

まず、本発明の前提に係わる提供されるサービスの概略を説明しておく。例えば、依頼人Aは、（１）インターネットに接続された自己のWWW（World Wide Web）サーバに格納されたホームページが、インターネット上で相当期間公開されていることを記録すること、及び（２）ホームページの存在及びその存在場所を公衆が知り得るようになるため当該ホームページにリンクを貼ることを、本サービスの提供者Bに依頼する、ものとする。

本依頼を受けたサービス提供者Bは、依頼人Aの知らない任意のタイミングで、指定されたURLのホームページに、依頼人Aの知らないIPアドレスからアクセスし、当該ホームページをコピーする。次に、サービス提供者Bは、ホームページのURL及びアクセス元のIP（Internet Protocol）アドレス等を含む属性情報を生成し、ホームページのコピー及びその属性情報を、日時と共にユニークに特定し且つ認証する電子証明書を取得する。そして、サービス提供者Bは、ホームページのコピー及び属性情報と、取得した電子証明書とを対応付けて保存する。

サービス提供者Bは、依頼人Aの知らない任意のタイミングで、再度指定されたURLのホームページにアクセスし、当該ホームページをコピーする。この際、アクセス元のIPアドレスを変更してアクセスすることにより、依頼人AのWWWサーバがアクセス制限をしていないという証明を付加的に得ることができる。次に、サービス提供者Bは、上と同じように属性情報を生成し、ホームページのコピー及びその属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得する。そして、サービス提供者Bは、ホームページのコピー及び属性情報と、取得した電子証明書とを対応付けて保存する。サービス提供者Bは、このような処理を依頼人Aの指定した相当期間繰り返す。

また、サービス提供者Bは、（２）の依頼に対し、指定されたホームページのURLへのリンクをインターネットに接続された自己のWWWサーバのホームページに掲載し、一般公衆がアクセス可能にする。例えば、当該リンクを、依頼人ごと、又は内容の分野毎に検索できるようにしておく場合もある。なお、WWWサーバにリンクを掲載していたことについても掲載期間等と共に記録を残してお



く。

依頼人 A は、上の依頼と同時に又は必要となった時に、上の（１）で指定したホームページに対する記録内容の提供をサービス提供者 B に申し込むことができる。この申込みに対応してサービス提供者 B は、保存したホームページのコピー及び属性情報と電子証明書とを依頼人 A に提供する。この際、例えば C D - R 等に上で述べたデータを書き込んで提供することも可能であるし、インターネットを介して提供することも可能である。さらに、上の（２）の結果として、サービス提供者 B の WWW サーバに、指定したホームページへのリンクが掲載されていたこと及びその期間等についての記録を証明書として、依頼人 A に提供する場合もある。

依頼人 A は、サービス提供者 B から提供を受けた情報を当該ホームページがインターネット上で相当期間公開していたことの証明として使用することができる。

#### 【 0 0 0 8 】

依頼人 A は、上で述べた（１）及び（２）の他に、（３）インターネット上の一般公衆向け検索エンジンで、指定したホームページが検索できるということの記録をサービス提供者 B に依頼することもできる。これは、ホームページの存在及び存在場所を公衆がより知り易い状態にあったことの証拠となる。サービス提供者 B は、任意の検索エンジンで、適切なキーワード等で検索を行う。指定されたホームページが検索できた場合には、当該検索できたという事実及び使用した検索エンジンのアドレス及び名称、並びに使用したキーワード、検索日時等を記録する。この記録を証明書として、記録内容提供依頼に応じて、依頼人 A に提供する場合もある。

依頼人 A は、（１）では自己の WWW サーバに格納されたホームページについて記録することを依頼していたが、（１）' 他人の WWW サーバに格納されたホームページについて記録することをサービス提供者 B に依頼できる。この場合、サービス提供者 B は上の（１）で述べたような処理を同じように実施する。しかし、他人の WWW サーバのホームページが、依頼人 A の指定した相当期間中存在し続ける保証は無く、存在しなくなってしまうたり、改変される場合もある。存

在しなくなってしまった場合には、サービス提供者Bは、インターネット上で公開が確認された期間を記録し、依頼人Aの記録内容提供依頼に応じて、通常提供する情報に加え当該期間を提供する場合もある。改変される場合には、上で述べた処理を実施すれば、改変の履歴が残る。なお、他人のWWWサーバに格納されたホームページは、依頼人AがそのURLを指定してもよいし、例えば指定された検索エンジンで指定されたキーワード検索を行った結果の全てのURLといった指定も可能である。

また、依頼人Aは、(4) 自己又は他人のWWWサーバに格納されたホームページのバージョン遷移の記録をサービス提供者Bに依頼することもできる。サービス提供者Bは、(1) と同じ処理を実施する。但し、サービス提供者Bは、前回アクセスした時のホームページの内容と、今回アクセスした時のホームページの内容とが異なるかを検査する。異なる場合には、例えば、以前と異なっていたということを記録する。

なお、サービス提供者Bがホームページのコピーを保存する必要は無い。例えば依頼人Aが保存すれば良い。サービス提供者Bがホームページのコピーを保存しない場合には、(1) 及び(1)'の処理でアクセス毎に保存されるのは、属性情報と電子証明書だけである。また、(4) の場合、前回アクセスした時のホームページの内容と今回アクセスした時のホームページの内容が異なっていた場合、その差分を保存する又は異なっていた場合にのみホームページ全体を保存する等により、バージョンの変更を保存することができる。

また(1) 及び(1)'の記録依頼における記録期間、回数、頻度等は、依頼人Aにより指定できる。サービス提供者Bはそれに従って記録を行う。

さらに、(2) 乃至(4) のサービスはオプションとすることができ、特に(2) 及び(3) といったサービスは、他の媒体等でホームページの存在及び所在が公衆に明らかになっていれば必要ない。

#### 【0009】

一方サービス提供者Bは、本サービスを続けていくと、インターネットを介して公開されていたという電子証明書付きのホームページを多数保持することになる。この情報を用いて、サービス提供者Bは、(5) 電子証明書付きのホームペ

ージ提供サービスを行うことができる。例えば、サービス提供者 B は、インターネットを介してキーワード検索等ができるようなデータベースを構築し、第 3 者に検索サービスを提供する。そして検索者 S の記録内容提供依頼に応じて、インターネットを介して又は C D - R のような媒体で、記録内容を提供する。また、電子証明書付きのホームページの要約を作成し、その要約で検索のスクリーニングができるような形態にデータベースを構築する場合もある。

以上のようなサービスを提供するための電子情報公開証明システムの概要を図 1 に示す。ネットワーク 1 には、3 で示すサーバ A、5 で示すサーバ B、7 で示すサーバ C、9 で示すサーバ D、1 1 で示すサーバ E 及び図示されない多数のコンピュータが接続されている。ネットワークである 1 は例えばインターネットである。3 で示すサーバ A は、WWW サーバであり、電子情報、例えば URL が <http://www.abcd.co.jp> であるホームページ 3 1 を格納しており、ネットワーク 1 で公開している。

5 で示すサーバ B は、サービス提供者が管理するサーバであり、依頼人指定の電子情報にアクセスし、コピーを取得するコピー取得機能 5 1 と、例えば URL 等の電子情報の所在に関する情報及びアクセス条件を含む属性情報を生成する属性情報生成機能 5 3 と、電子情報のコピー及び属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得する証明書取得機能 5 5 と、必要な情報を保存する保存機能 5 7 と、依頼人の申し出に対応して保存されている電子証明書等を提供するための証明書提供機能 5 9 とを含む。この 5 で示すサーバ B には記憶装置 6 1 が接続されている。

7 で示すサーバ C は、特定の電子情報を日時と共にユニークに特定し且つ認証する証明書を発行するタイムスタンプ証明書発行機能 7 1 を有している。7 で示すサーバ C は、ネットワーク 1 を介して証明書発行依頼を受け取り、タイムスタンプ証明書発行機能 7 1 にて電子証明書を発行し、依頼元に電子証明書を送り返す。

【 0 0 1 0 】

9 で示すサーバ D は、5 で示すサーバ B に機能を付加するためのサーバであって、例えば WWW サーバとして依頼人が指定したホームページへのリンク 9 1 を

掲載する。但し、このようなリンク 9 1 のデータベースを作成し、リンク先ホームページの内容又は所有者等毎に検索可能にしておく場合もある。さらに、5で示すサーバBに接続されている記憶装置 6 1 のデータを用いてデータベース 9 5を作成し、9で示すサーバDがこのデータベース 9 5をネットワークを介して検索可能にする検索機能 9 3を保持している場合もある。さらに、記憶装置 6 1 のデータから各電子情報の要約を作成し、この要約に関するデータベース 9 7を検索機能 9 3がネットワークを介して検索可能にする場合もある。

1 1で示すサーバEは、一般公衆向け検索エンジンである。この一般公衆向け検索エンジンは、従来と変わらないので説明は割愛する。

次に、本発明により提供されるサービスの概要 (1) 及び (1)' を、図 1 に示したシステムの動作として説明する。

依頼者 A は例えば 3 で示すサーバ A の URL <http://www.abcd.co.jp> のホームページを相当期間記録すべき電子情報として指定し、サービス (1) 又は (1)' をサービス提供者 B に依頼する。サービス提供者 B は 5 で示すサーバ B を用いて処理を行う。5 で示すサーバ B のコピー取得機能 5 1 は、任意のタイミングで図 1 のサーバ A に示した <http://www.abcd.co.jp> に例えばルート (A) によりアクセスし、ホームページ 3 1 のコピーを例えばルート (B) を介して取得する。コピーは、例えば 5 で示すサーバ B のメインメモリに保持される。コピー取得機能 5 1 は、アクセス毎に、アクセス元の IP アドレスを記憶装置に記憶しておく。コピー取得機能 5 1 は、アクセス条件を決定する機能を含んでおり、例えば依頼人が指定した相当期間中、どのタイミングで且つどのアクセス元 IP アドレスを使用してアクセスするか決定する。また、依頼人が頻度を指定している場合には、当該頻度の指定を満たすように、アクセスをスケジューリングする。

属性情報生成機能 5 3 は、このアクセス元の IP アドレスと依頼人 A 指定の URL とを含む属性情報を生成する。属性情報には、IP アドレス及び URL のほかに、例えば 5 で示すサーバ B が図示しないプロキシ・サーバを介してネットワーク 1 に接続している場合には、このプロキシ・サーバの IP アドレスや、アクセス日時を含むようにしてもよい。

【 0 0 1 1 】

証明書取得機能 5 5 は、取得したホームページ 3 1 のコピー及び生成した属性情報に対して電子証明書を取得する。より具体的な処理については後に詳述する。図 1 のシステムでは、証明書取得機能 5 5 は、ネットワーク 1 の例えばルート (C) を介して発せられる電子証明書発行依頼を、7 で示すサーバ C のタイムスタンプ証明書発行機能 7 1 にて受領し、タイムスタンプ証明書機能 7 1 により発行される電子証明書をネットワーク 1 の例えばルート (D) を介して受領する。タイムスタンプ証明書発行機能 7 1 については後に詳しく述べるものとする。

保存機能 5 7 は、コピー取得機能 5 1 が取得したホームページ 3 1 のコピーと、属性情報生成機能 5 3 が生成した属性情報と、証明書取得機能 5 5 が取得した電子証明書とを、記憶装置 6 1 に格納する。但し、コピー取得機能 5 1 が取得したホームページ 3 1 のコピーを保存することは任意である。例えば、依頼人 A が自分で保存する場合もあるからである。また、保存機能 5 7 は、前回コピーしたホームページ 3 1 の内容と、今回アクセスしたホームページ 3 1 の内容が同一である場合、今回取得したホームページ 3 1 のコピーを保存しないといった判断を行うようにしてもよい。また、保存機能 5 7 は、後に証明書提供機能 5 9 が必要なデータを取り出し易いように、依頼人毎又は指定された URL 毎にデータを保存しておく。

記録依頼と同時に又は任意のタイミングで依頼人 A は記録内容の提供を申し出る。この際、証明書提供機能 5 9 は、それに応じて、依頼の対象となるホームページ 3 1 のコピー、属性情報及び電子証明書を記憶装置 6 1 から読み出し、図 1 の例では CD-R 6 3 等の記憶媒体に格納して、依頼人 A に提供する。なお、ホームページ 3 1 のコピー、属性情報及び電子証明書は、アクセス毎に記憶されるが、証明書提供機能 5 9 はこれらを全て CD-R 等の記憶媒体に格納して提供してもよいし、ホームページ 3 1 のコピーに変化がない場合には、最初のアクセス時のホームページ 3 1 のコピーと全ての属性情報及び全ての電子証明書を提供するようにしてもよい。さらに、証明書提供機能 5 9 において、属性情報及び電子証明書を用いて、URL、アクセス元 IP アドレス及び証明書日時を含むアクセス記録を作成し、当該アクセス記録と、最初のアクセス時のホームページ 3 1 と、全ての属性情報と、全ての電子証明書とをサービス提供者 B による証明書として

○

提供するようにすることも可能である。なお、保存機能 5 7 がホームページ 3 1 のコピーを保存しない場合には、当然証明書提供機能 5 9 も依頼人 A にホームページ 3 1 のコピーを提供しない。

【0 0 1 2】

次に、本発明により提供されるサービスの概要（2）を、図 1 に示したシステムに基づき説明する。（2）は、ホームページの存在及びその存在場所を公衆が知り得るようにするため当該ホームページにリンクを貼ることを、依頼人 A がサービス提供者 B に依頼するものである。

この依頼に応じてサービス提供者 B は、ネットワーク 1 に接続された 9 で示すサーバ D に、3 で示すサーバ A に格納されたホームページ 3 1 へのリンク 9 1 を掲載する。依頼数が少なければ、9 で示すサーバ D に格納されたホームページに、単に指定されたホームページの URL を掲載するだけでも良い。しかし、依頼数が多い場合には、リンクについてのデータベースを構築し、ネットワーク 1 を介して、第三者が、ホームページの内容又は依頼人の業種等によって検索できるようにする場合もある。サービス提供者 B は、ホームページ 3 1 へのリンク 9 1 を自己のホームページに掲載していた期間や、検索可能であった期間を記憶装置に記録しておき、後に依頼人 A 等から求められた時には、当該記録を証明書として提供する。

次に、本発明により提供されるサービスの概要（3）を、図 1 に示したシステムに基づき説明する。（3）は、ネットワーク 1 上の一般公衆向け検索エンジンである 1 1 で示すサーバ E で、指定したホームページが検索できるということの記録をサービス提供者 B に依頼をするものである。

サービス提供者 B は、例えば 5 で示すサーバ B を介して、1 1 で示すサーバ E における検索エンジンで、適切なキーワード等により検索を行い、指定されたホームページ 3 1 が検索できた場合には、当該検索できたという事実及び 1 1 で示すサーバ E の名称及びアドレス、使用したキーワード、検索日時等を記録する。後に依頼人 A 等から求められた時には、この記録を証明書として提供する。

次に、本発明により提供されるサービスの概要（4）を、図 1 に示したシステムに基づき説明する。（4）は、ホームページ 3 1 のバージョン遷移の記録をサ

ービス提供者Bに依頼するものである。

サービス提供者Bは、5で示すサーバBを用いて(1)と同様な処理を行う。すなわち、所定のタイミングで3で示すサーバAのホームページ31にアクセスし、ホームページ31のコピーを取得する。次に、URL及びアクセス条件を含む属性情報を生成し、属性情報及びホームページ31のコピーに対し電子証明書を取得する。そして、少なくとも属性情報及び電子証明書を記憶装置61に保存する。ホームページ31のコピーを記憶装置に保存するようにすることも可能である。次に、所定のタイミングにて3で示すサーバAのホームページ31にアクセスし、同様な処理を行い、属性情報及びホームページ31のコピーに対し電子証明書を取得する。そして、前回アクセスした時のホームページ31、より正確には、最も最近変更が検出された時のホームページ31、の内容と、今回アクセスした時のホームページ31の内容が異なっているか判断する。この判断は、コピー取得機能51が行っても、保存機能57が行ってもかまわない。内容が異なっている場合には、少なくとも属性情報及び電子証明書に加え、異なっていたということを記憶装置に記録する。場合によっては、前回アクセスした時のホームページ31の内容と今回アクセスした時のホームページ31の内容の差分を記憶装置に記録するようにしてもよいし、異なっている場合には、必ずホームページ31の全体のコピーを記憶装置に保存するようにしてもよい。

依頼人A等から求められたときには、サービス提供者Bは、証明書提供機能59により、少なくとも属性情報及び電子証明書と変更の有無の記録を提供する。差分や異なる毎にホームページ全体を提供してもよい。

#### 【0013】

次に、本発明により提供されるサービスの概要(5)を、図1に示したシステムに基づき説明する。(5)は、電子証明書付のホームページ提供サービスである。

サービス提供者Bは、9で示すサーバDに検索機能93を設け、記憶装置61に蓄えられた電子証明書及び属性情報付きのホームページ31のコピーを使用して、データベース95を作成する。そして、第三者に検索機能93からデータベース95を検索できるようにする。第三者が使用を欲するホームページ31のコ

ピーを見つけた場合には、ネットワーク 1 等を介して、記録内容提供依頼をサービス提供者 B に提出する。サービス提供者 B は、証明書提供機能 5 9 を使用して、例えば C D - R 6 3 等に提供を求められたホームページ 3 1 のコピー及び属性情報並びに電子証明書を格納し、当該 C D - R 6 3 等を提供する。ネットワーク 1 を介して上述のようなデータを送信するようにしてもよい。

さらに、サービス提供者 B は、ホームページ 3 1 のコピーからその要約を作成し、要約のデータベース 9 7 を構築し、検索機能 9 3 により第三者が検索可能にすることも可能である。第三者は、要約のデータベースでスクリーニングをしたのちに、ホームページ 3 1 のコピーを確認し、必要な電子情報の記録内容提供依頼を出すことができるようになる。

本発明の主要なサービス ( 1 ) 及び ( 1 ) ' の処理フローを図 2 にまとめた。依頼人 A から、例えばホームページ等の記録対象電子情報に関する、例えば U R L 等の所在に関する情報及び例えば記録期間等の記録条件を指定した記録依頼がサービス提供者 B に提出された場合 ( ステップ S 1 ) には、記録条件に合致するようにコピー取得機能 5 1 は、アクセス条件を決定 ( ステップ S 3 ) し、当該 U R L に所定のタイミングで所定のアクセス元 I P アドレスからアクセスして、ホームページのコピーを取得 ( ステップ S 5 ) する。そして、属性情報生成機能 5 3 は、ホームページの U R L とアクセスの条件としてアクセス元 I P アドレスを含む属性情報を生成 ( ステップ S 7 ) する。

その後、証明書取得機能 5 5 は、属性情報及び取得したホームページのコピーを日時と共に特定し且つ認証する電子証明書を、タイムスタンプ証明書発行機能 7 1 から取得 ( ステップ S 9 ) する。なお、5 で示すサーバ B が、タイムスタンプ証明書発行機能 7 1 を含むような構成とすることも可能であって、その場合証明書取得機能 5 5 はタイムスタンプ証明書発行機能 7 1 に置き換えられる。

そして、保存機能 5 7 は、少なくとも属性情報及び電子証明書を記憶装置 6 1 に格納 ( ステップ S 1 1 ) する。なお、上でも述べたが、ホームページのコピーを記憶装置に保存するかは任意である。そして、この処理を記録終了の条件が満たされるまで繰り返す ( ステップ S 1 3 ) 。記録終了の条件とは、例えば依頼人 A の指定した記録期間が終了した場合や、依頼人 A の指定した記録回数に達した



場合等である。

【0014】

図3に本発明の主要なサービス(1)及び(1)'に加え(4)のサービスを合わせて行う場合の処理フローの一例を示す。

依頼人Aから、例えばホームページ等の記録対象電子情報の、例えばURL等の所在に関する情報及び例えば記録期間等の記録条件を指定した記録依頼がサービス提供者Bに提出された場合(ステップS21)に、記録条件に合致するようにコピー取得機能51は、アクセス条件を決定(ステップS23)し、当該URLに所定のタイミングで所定のアクセス元IPアドレスからアクセスして、ホームページのコピーを取得(ステップS25)する。そして、属性情報生成機能53は、ホームページのURLとアクセスの条件としてアクセス元IPアドレスとを含む属性情報を生成(ステップS27)する。

その後、証明書取得機能55は、属性情報及び取得したホームページのコピーを日時と共に特定し且つ認証する電子証明書を、タイムスタンプ証明書発行機能71から取得(ステップS29)する。なお、5で示すサーバBが、タイムスタンプ証明書発行機能71を含むような構成とすることも可能である。

ここでは次に保存機能57が、前回アクセスした時のホームページの内容と、今回アクセスした時のホームページの内容に変更が無いか検査(ステップS31)する。この検査は、記憶装置61に格納された最も最近変更が検出された時のホームページのコピーを読み出し、今回アクセス時のホームページのコピーとを比較することにより行われる。変更を検出した場合には、ホームページのコピーと電子証明書と属性情報とを関連付けて記憶装置に保存(ステップS33)する。一方、変更が検出されない場合には、証明書及び属性情報を記憶装置に保存(ステップS35)する。このような処理が記録終了の条件が満たされるまで繰り返される(ステップS37)。

図3のような処理フローが行われたときには、例えば図4のような情報が保存されることになり、指定されたURLのホームページの遷移を証明することができる。図4で、初回のアクセス時には、全て変更ということで、ホームページのコピーと電子証明書と属性情報とを記憶装置に保存する。二回目のアクセス時に

は、初回のアクセス時に保存したホームページのコピーと今回アクセスした時に取得したホームページのコピーを比較し、変更が無いと判断され、電子証明書及び属性情報のみが保存される。三回目のアクセス時には、初回のアクセス時に保存したホームページのコピーと今回アクセスした時に取得したホームページのコピーを比較し、変更が無いと判断され、電子証明書及び属性情報のみが保存される。四回目のアクセス時には、初回のアクセス時に保存したホームページのコピーと今回アクセスした時に取得したホームページのコピーを比較し、変更があると判断され、四回目のアクセス時に取得したホームページのコピーと、電子証明書と、属性情報とが保存される。以下同様な処理が変更あり又は無しの場合に行われる。比較の対象は、最も最近の変更を検出したため保存を実行したホームページのコピーとなる。

【 0 0 1 5 】

次に依頼人 A による記録内容提供依頼に応じて実行される処理フローの例を図 5 に示す。記録内容提供依頼（ステップ S 4 1）には対象となる電子情報が含まれているので、まず証明書提供機能 5 9 は、対象となる電子情報を特定（ステップ S 4 3）する。そして、証明書提供機能 5 9 は、記憶装置 6 1 から対象電子情報のコピーと、電子証明書及び属性情報を読み出す（ステップ S 4 5）。なお、記録依頼が 1 回だけの記録を要求していたり、結果的に 1 回アクセスしただけで対象電子情報が無くなったりする場合には、読み出されるデータは 1 セットのみであるが、通常複数回に渡って記録しているので、電子情報のコピーと属性情報と電子証明書のセットを複数読み出すことになる。

そして、証明書提供機能 5 9 は、公開期間の計算を付加的に行う（ステップ S 4 7）。電子証明書には日時の記録が含まれるので、初回アクセス時に取得した電子証明書と最後にアクセスした時に取得した電子証明書を参照すれば、少なくともいつからいつまで公開されていたか分かるので、この情報を公開期間とする。但し、この処理は任意である。

最後に、証明書提供機能 5 9 は、対象電子情報のコピーと、電子証明書及び属性情報、並びに公開期間情報を、例えば C D - R 等の媒体に格納して提供（ステップ S 4 9）する。

## 【 0 0 1 6 】

ここで電子証明書について図 6 を用いて簡単に説明しておく。本発明では、電子情報を日時と共にユニークに特定し且つ認証する電子証明書を発行するものであれば、どのような方式にて電子証明書を発行してもよい。よって、以下の説明は一例であって、他の方式にて電子証明書を発行することにしてもかまわない。

電子情報 1 0 1 を電子証明書の対象であるとする、まず、電子情報 1 0 1 に対してハッシュ値 1 0 3 を計算する。ハッシュ関数は一方向関数であれば何でも良い。ハッシュ値の計算までを例えば証明書取得機能 5 5 が行う。そして、このハッシュ値 1 0 3 を含む証明書発行依頼を、タイムスタンプ証明書発行機能 7 1 に送る。タイムスタンプ証明書発行機能 7 1 は、同じように送られてきた他のハッシュ値と共に処理をする。例えば図 6 のように、2 つのハッシュ値からもう一つのハッシュ値を生成するといった処理を繰り返し、送られてきた全ハッシュ値から最終的に一つのハッシュ値 1 0 6 を生成する。このハッシュ値 1 0 6 と、時刻  $T-1$  ( $T$  は整数) における SHV (Super Hash Value: スーパー・ハッシュ値) 1 0 5 とを用いて時刻  $T$  における SHV 1 0 7 を生成する。このようにして生成された時刻  $T$  における SHV 1 0 7 とハッシュ値 1 0 3 と、時刻  $T$  の時刻情報と、文書 ID とが電子証明書 1 0 9 を構成する。この電子証明書 1 0 9 はハッシュ値 1 0 3 の送り主に送信され、電子情報 1 0 1 と電子証明書 1 0 9 とを対にして、電子情報 1 0 1 を日時と共にユニークに特定し且つ認証することができるようになる。

なお、電子情報であるホームページを図 6 の電子情報とする場合には、HTML 文書が電子情報に当たる。よって、図 7 に示したように、HTML 文書 1 1 0 と、URL 及びアクセス元 IP アドレスなどを含む属性情報 1 1 1 とからハッシュ値を計算し、このハッシュ値から電子証明書を作成することになる。但し、ホームページの内容が文章だけであればこれで十分であるが、通常ホームページには例えば GIF ファイル等の画像ファイル 1 1 2 が埋め込まれている。このような場合には、GIF ファイル等の画像ファイルの内容もネットワーク上で公開されていた情報に含まれるため、この画像ファイルと、HTML 文書と、属性情報とからハッシュ値を計算するようにする。

さらに、HTML文書に埋め込まれているのは、静止画像のみならず、動画像であったり、サウンドであったり、ブラウザのプラグイン等を必要とするフォーマットのファイルであったり、Java (Sun Microsystems社の商標) アプレットであったりする。このようなオブジェクトが埋め込まれている場合には、これらのオブジェクトについても指定URLアクセス時にコピーし、ハッシュ値計算に用いる。ハッシュ値を個々のファイルごとに計算しても、全てのファイルについて1つ計算してもよい。

## 【0017】

このように本発明のサービスの概要(1)及び(1)'により、ネットワーク上で公開された電子情報に対し、公開されていたことを証明することができるようになる。(2)及び(3)により、一般公衆にその電子情報の存在及びその所在を知られるようになっていたことを証明することができるようになる。また、(4)により、電子情報のバージョン遷移を把握することができるようになる。さらに、(5)により、サービス提供者は電子証明書付き電子情報をより有効に使用することができ、依頼人は電子情報の公衆の利用を促進でき、第三者は自己が保持していなかった証拠力のある電子情報を取得することができるようになる。

このようなシステムにて、例えば特許の分野においては、属性情報及び電子証明書付き電子情報を、特許異議申立てや無効審判の証拠に使用することができるようになる。また、自己のホームページ等を公開情報のように用いることができるようになる。また、新規性の喪失の例外適用の証拠としても使用することができる。

以上述べた内容は一例であって様々な変形が可能である。例えば、5で示したサーバBに含まれる5つの機能は、図1では1つのサーバに含まれるように示しているが、複数のサーバに分けて存在するようにすることも可能である。同様に、9で示したサーバDでは、依頼されたホームページへのリンクを掲載し、且つ検索機能を設けているが、これらも別個のサーバにて実施されるようにすることも可能である。ネットワーク1に接続される一般公衆向け検索エンジンは1つに限定されない。また、httpに限定されず、ftpでも対応することができる。

。 7 で示したサーバ C の機能を 5 で示したサーバ B の機能に含めることも可能である。 7 で示したサーバ C によるサービスを行う主体と、 5 で示したサーバ B によるサービスを行う主体は、別でも同一でもよい。ネットワーク 1 はインターネットに限定されず、他の非排他的なアクセスを許可するネットワーク及びネットワーク利用を希望する者が非排他的に取り扱われるネットワークにまで拡大可能である。記録内容提供のための媒体を C D - R 6 3 としていたが、これも一例であって他の媒体、例えば C D - R O M でも、 D V D でもよい。

また図 1 に示した機能ブロックの分け方は一例であって、 1 つの機能ブロックを複数の機能ブロックに分けることも、複数の機能ブロックを 1 つの機能ブロックにまとめることも可能である。図 1 に示した機能ブロックの機能を実現するプログラムとコンピュータの組み合わせにより図 1 のような装置を構成することも、一部又は全部を専用の電子回路等により実施することも可能である。

【 0 0 1 8 】

【発明の効果】

インターネット等のネットワーク上で、特定の電子情報が所定の条件の下公開されていたことを証明するための方法、システム及びコンピュータ・プログラム並びに該コンピュータ・プログラムを格納した記録媒体を提供することができた。

【図面の簡単な説明】

【図 1】

本発明におけるシステムの概要を示すブロック図である。

【図 2】

電子情報記録依頼に応じて行われる処理の一例を示すフローチャートである。

【図 3】

電子情報記録依頼に応じて行われる処理の一例を示すフローチャートである。

【図 4】

電子情報にアクセスするごとに保存する情報の種類の一例を示す模式図である。

【図 5】

記録内容提供依頼に応じて行われる処理の一例を示すフローチャートである。

【図 6】

電子情報を日時と共に特定し且つ認証する電子証明書の発行処理の一例を示す模式図である。

【図 7】

図 6 の発行処理にて行われるハッシュ値の生成について説明するための模式図である。

【符号の説明】

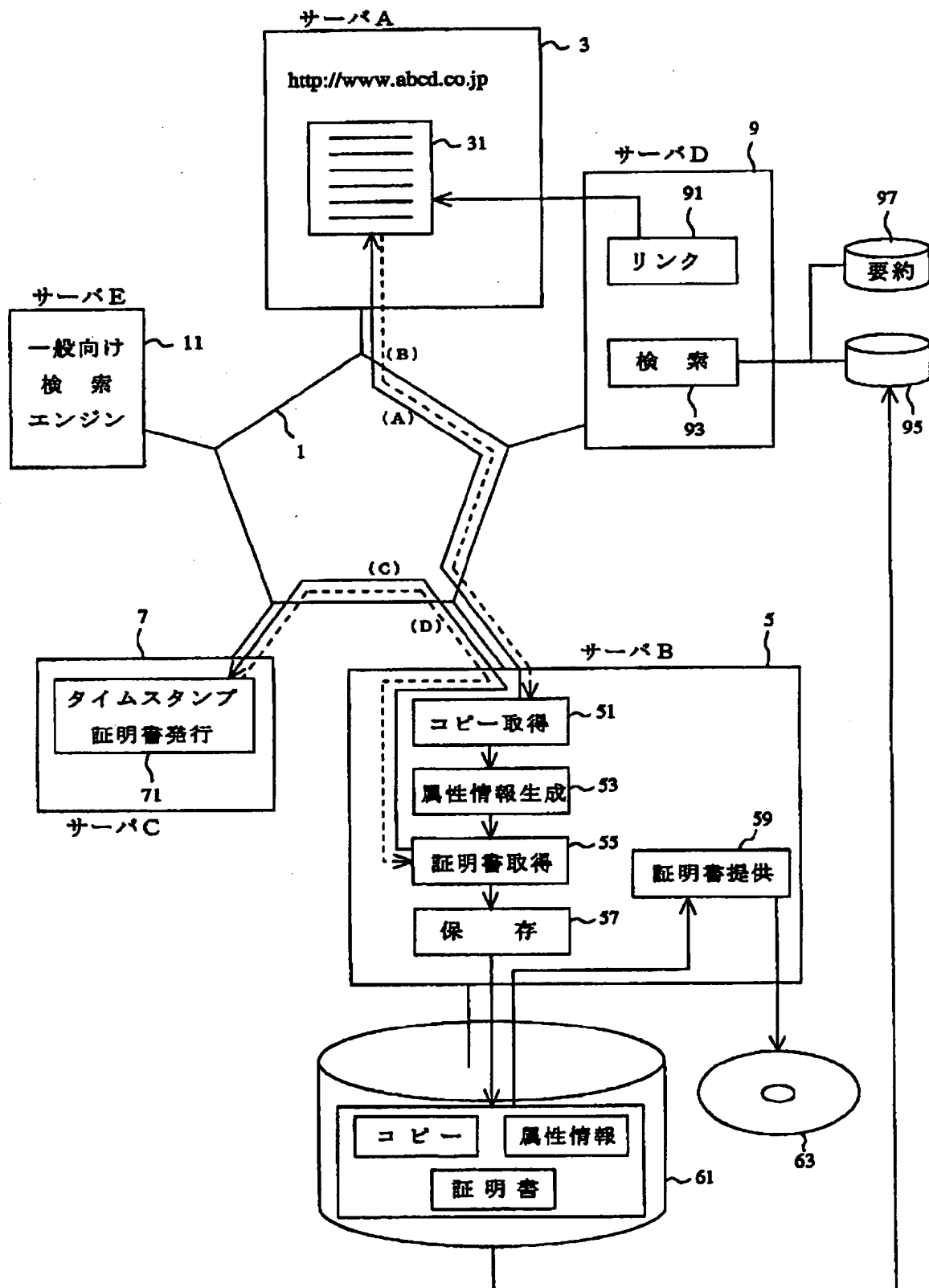
- 1 : ネットワーク
- 3 : サーバ A
- 5 : サーバ B
- 7 : サーバ C
- 9 : サーバ D
- 1 1 : サーバ E
- 3 1 : ホームページ
- 5 1 : コピー取得機能
- 5 3 : 属性情報生成機能
- 5 5 : 証明書取得機能
- 5 7 : 保存機能
- 5 9 : 証明書提供機能
- 6 1 : 記憶装置
- 6 3 : C D - R
- 7 1 : タイムスタンプ証明書発行機能
- 9 1 : リンク
- 9 3 : 検索機能
- 9 7 : 要約データベース
- 1 0 1 : 電子情報
- 1 0 3 : ハッシュ値
- 1 0 5 : 時刻 T - 1 における S H V

- 1 0 6 : ハッシュ値
- 1 0 7 : 時刻 T における S H V
- 1 0 9 : 電子証明書
- 1 1 0 : HTML 文書
- 1 1 1 : 属性情報
- 1 1 2 : 画像ファイル

【書類名】

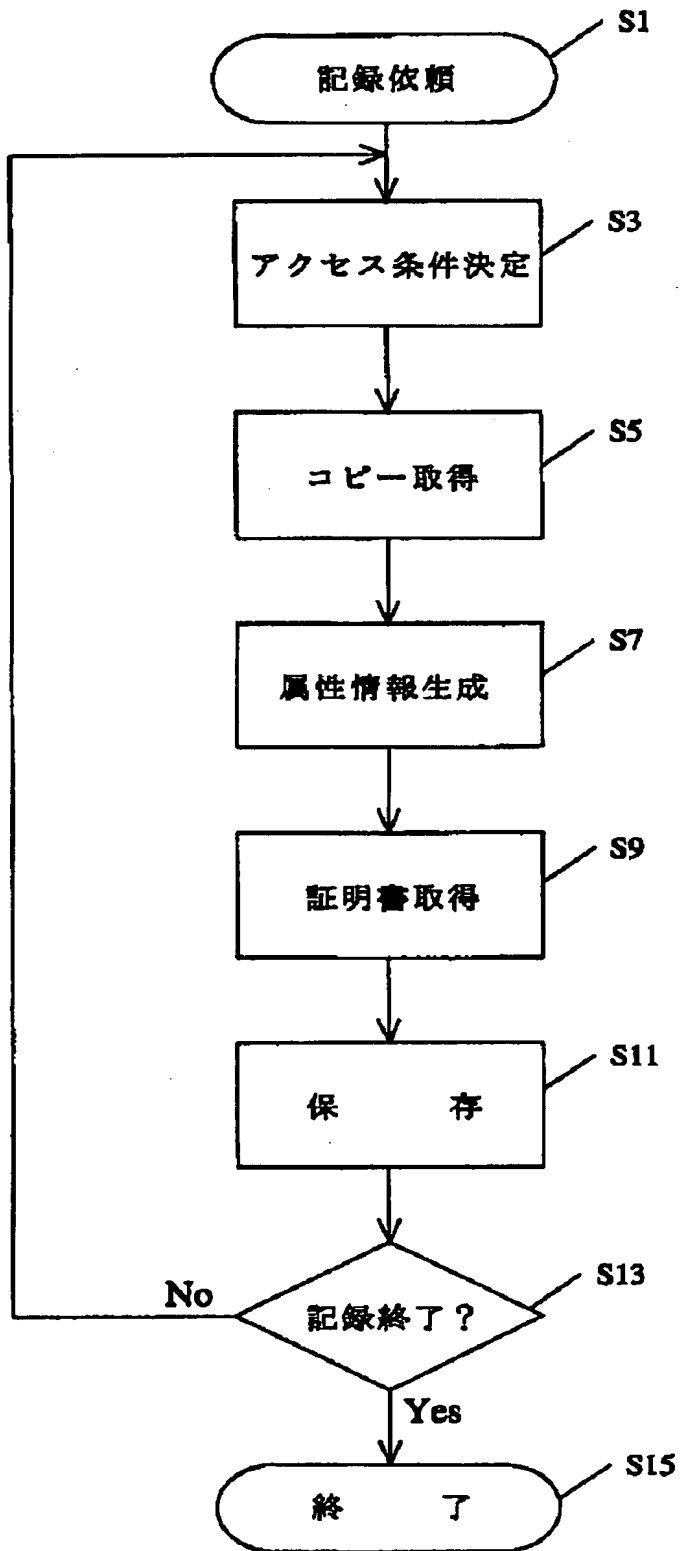
図面

【図 1】

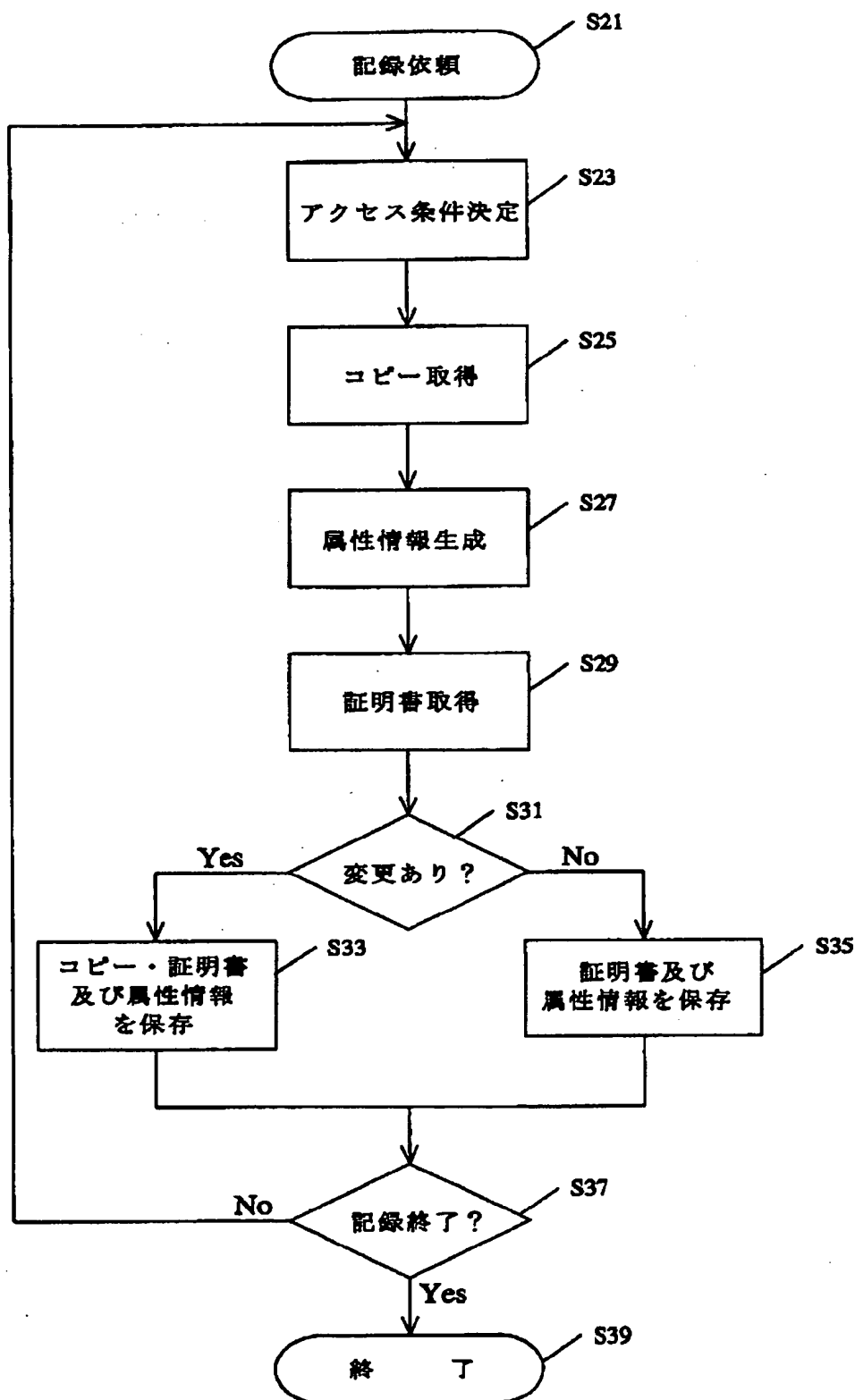




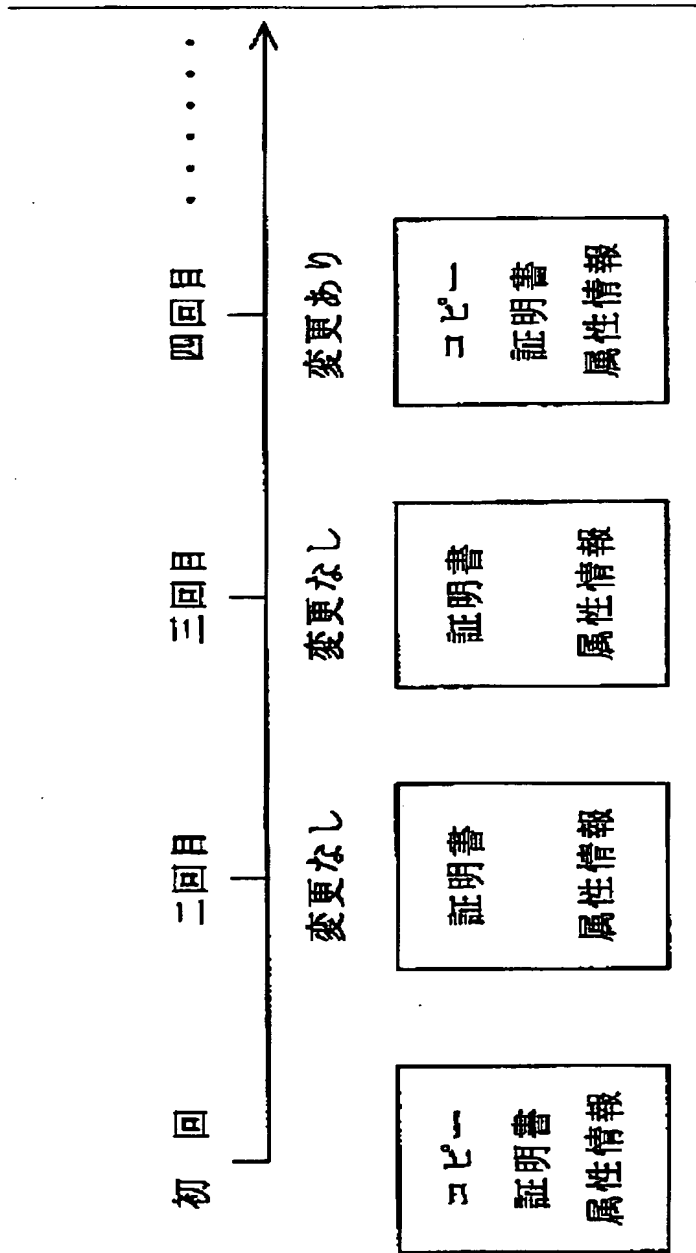
【図 2】



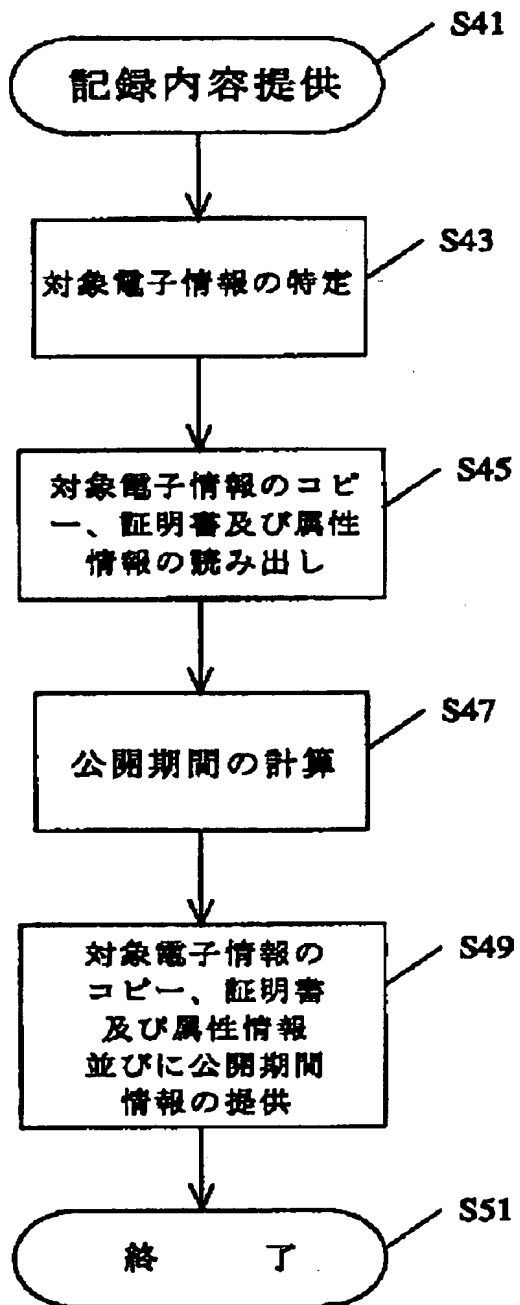
【図 3】



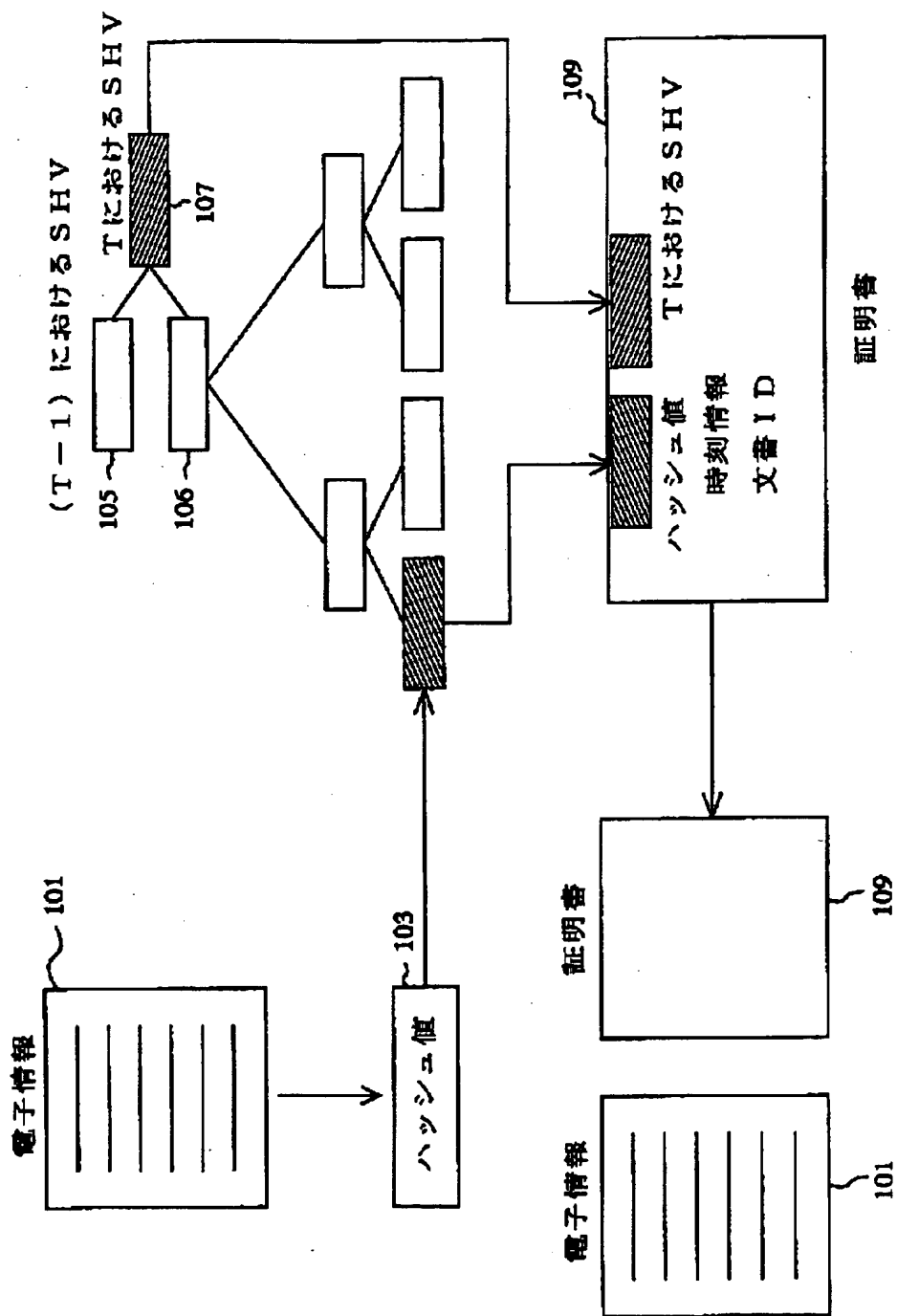
【図 4】



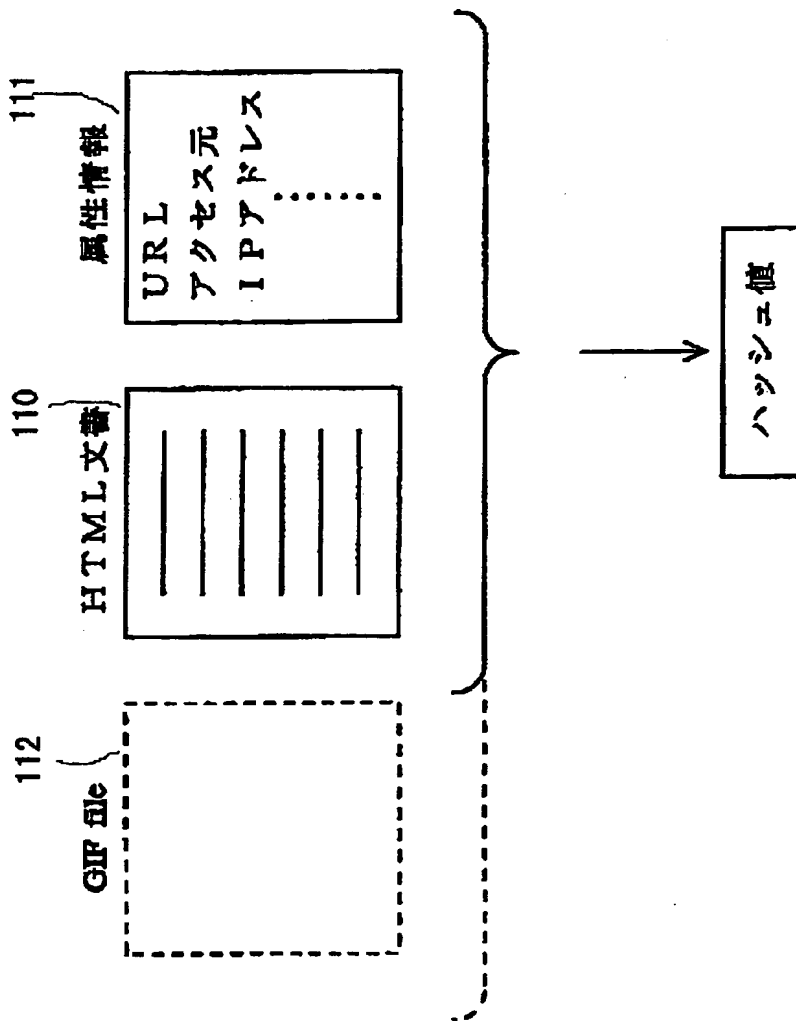
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 インターネット等のネットワーク上で、ある電子情報が所定の条件の下公開されていたことを証明する。

【解決手段】 サービス提供者 B は、依頼人 A から指定された URL のホームページにアクセスし、当該ホームページをコピーし、URL 及びアクセス元の IP アドレス等を含む属性情報を生成し、ホームページのコピー及びその属性情報を、日時と共にユニークに特定し且つ認証する電子証明書を取得し、ホームページのコピー及び属性情報と対応付けて保存する。これを指定された期間繰り返す。依頼人 A は、依頼と同時に又は必要となった時に、指定したホームページに対する記録内容の提供をサービス提供者 B に申し込むことができる。この申込みに対応してサービス提供者 B は、保存したホームページのコピー及び属性情報と電子証明書とを依頼人 A に提供する。また、サービス提供者 B の WWW サーバに、指定したホームページへのリンクが掲載されていたこと及びその期間等についての記録を証明書として、依頼人 A に提供する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 6 7 4 7 ]

1. 変更年月日	1 9 9 0 年 8 月 2 4 日
[変更理由]	新規登録
住 所	東京都大田区中馬込 1 丁目 3 番 6 号
氏 名	株式会社リコー